Codes With Parity Conditions on Subsets of Coordinates

E. C. Posner
Office of Telecommunications and Data Acquisition

Z. Reichstein
Harvard University, Graduate Student

This article considers binary codes with the constraint that the codes restricted to certain subsets of columns must be contained in particular codes of the shorter lengths. In particular, we consider codes of even length 2k, and of minimum distance $\geq d$, where the code obtained by restricting to the first k positions has even weight and at the same time the code obtained by restricting to the last k positions also has even weight. If $k = 2n$, n odd, and $d = 2n$, we prove that the code has at most $8n - 4$ codewords, and $8n - 4$ is attainable for $n = 3$. This yields 20 binary words of length 12, distance ≥ 6, where the number of 1's in the first six and the last six positions is even for every codeword in the code. This permits a file-transfer protocol control function assignment for personal computers to be chosen for 20 control functions using essentially just pairs of upper-case alphabetic ASCII characters where the Hamming distance between the binary forms of every two different control functions is at least six.

I. Introduction

In Ref. 1, the following problem was suggested: Find codes of the largest possible size with specified length and minimum Hamming distance where the shorter codes obtained by projecting the coordinates corresponding to a given partition of the coordinates are required to be contained in specified shorter codes. The examples in this paper require that the projection onto the first k coordinates must have even weight and similarity for the last k, where the length is $2k$.

The problem arose because simple file-transfer protocols for personal computers may have to be restricted for interbrand compatability to just ASCII binary eight-tuples corresponding to upper-case alphabetic characters, to avoid control characters that would be interpreted differently by machines of different manufacturers. Although the ASCII code is 8 bits, two of the bits are constant on the set of upper-case letters, and a third bit is parity. Hence, upper-case ASCII can be thought of as (26 of the 32) six-tuples of even weight. If we want control functions of two ASCII characters each, ignoring the constant 4 bits of the 16, our binary twelve-tuples are to have even weight in the first six positions and in the last, and we may want good distance properties to at least detect errors on noisy analog voice circuits. For example, we may want distance ≥ 6, where the maximum distance possible is of course 12. Subject to the above, we find that a code of 20 codewords exists, and that this is the largest code possible with the above constraints.

The above result is a special case of the main result of this paper. Namely, for k an integer $\geqslant 1$, let:

(1) $A(2k, d)$ be the largest size of a binary code of length $2k$ and minimum distance $\geqslant d$;

(2) $B(2k, d)$ be the same as (a) but each codeword has an even number of 1's in its first k columns *and* in its last k columns;

(3) $C(2k, d)$ is the same as (a) but each codeword has an even number of 1's.

We see that, in general, for trivial reasons,

$$B(2k, d) \leqslant C(2k, d) \leqslant A(2k, d)$$

The function A is, of course, well known; the function B is much more interesting than C and is the main focus of this paper. (The C-values are trivially obtained from the A-values.) Above we said that we show $B(12, 6) = 20$. We will also show that for $k = 2n$, n odd, $B(4n, 2n) \leqslant 8n - 4$, where $B(12, 6)$ is the case $n = 3$. We present evidence that the $8n - 4$ bound is the "right" one; if it fails for a certain n it is probably because certain Hadamard Matrices do not exist. We will also exhibit exact values or at least the tightest bounds we can for $B(2k, d)$ and $C(2k, d)$ for specific small values of k and d, and compare them with the well-known code sizes $A(2k, d)$ obtained from published tables of error-correcting codes.

II. Specific Values of *A*, *B*, and *C*

This section presents a table of the A, B, and C functions for lengths $2k$ up to 12 and all relevant d. Various techniques are used, some relying on later sections of this paper. The results are illustrated in Table 1. For simplicity, we call the A-function the *unconstrained* problem, the C-function the *even* problem, and the B-function the *even-even* problem. The most interesting even-even problems arise when the length is a multiple of 4, because then the code can contain antipodal codewords. References are given unless the result is obvious by inspection. Unreferenced values of A are taken from Ref. 2. Derivation of the results follow.

(1) $B(10, 4) = 32$. If $B(10, 4) > 32$, there would be three "head" five-tuples with different "tails" in the code. The tails form a code of length 5, minimum distance $\geqslant 4$, but $A(5, 4) = 2$, not 3. So $B(10, 4) \leqslant 32$.

Here's how to get 32 even-even codewords of length 10 and mutual distance $\geqslant 4$, proving $B(10, 4) = 32$. Consider the length-five linear code of two elements 00000 and 11110, at distance 4. Calling this code G_1, let $G_2, \cdots, G_7$ be the seven other cosets of G_1 in the vector space (group) of five-tuples of even weight. G_1 is of dimension 4, so there are indeed eight cosets altogether. Our desired code is the set of $32 = 8 \times 2 \times 2$ even-even ten-tuples $\alpha_{ijk} = (\beta_{ij}, \beta_{ik})$, $1 \leqslant i \leqslant 8$, $1 \leqslant j, k \leqslant 2$, where β_{ij} and β_{ik} are in G_i. Each G_i is, of course, a distance – 4 code, in its own right.

Now if $i_1 \neq i_2$, $d(\beta_{i_1 j}, \beta_{i_2 k}) \geqslant 2$, where d is Hamming distance. This is because $\beta_{i_2 j} \neq \beta_{i_2 k}$ if $i_1 \neq i_2$ because the cosets partition the space. And all nonzero distances are at least 2, being even. So $d(\alpha_{i_1 j_1 k_1}, \alpha_{i_2 j_2 k_2}) \geqslant 2 + 2 = 4$ if $i_1 \neq i_2$.

Finally, if $i_1 = i_2$, $d(\alpha_{ijk}, \alpha_{ij'k'}) \geqslant 4$ if $j' \neq j$ or $k' \neq k$, i.e., if the elements are distinct. For α_{ijk} differs from $\alpha_{ij'k'}$, in either head or tail (or both), and we have observed that each G_i is a distance-4 code. This completes the proof that $B(10, 4) = 32$.

(2) $B(10, 6) = 5$. The following five ten-tuples are at mutual distance 6 or greater:

00000	00000
11110	11000
11101	00110
00101	11011
10010	01111

This shows $B(10, 6) \geqslant 5$. We show $B(10, 6) \leqslant 5$ as follows. By complementing an even number of columns in each half, we can assume the all-0 word is in the code. If there were three left halves of weight 4, and so mutual distance 2, then right halves would be at mutual distance 4, contradicting $A(5, 4) = 2$. So there are at most two four-tuples on the left and two on the right. If there were six codewords, then there would be three two-tuples on the left (and on the right). Two of these heads are at distance 2, because $A(5, 4) = 2$. Their tails are at distance 4. But their tails are of weight 4, for the distance of the entire codeword from the 0 codeword is at least 6. Two five-tuples of weight 4 if different are at distance 2. So we do not have three two-tuples as heads, and $B(10, 6) \leqslant 5$.

(3) $B(12, 4) = 128$. There are $32 = 2^5$ distinct even-weight six-tuples from which to choose our heads and tails. If one even-weight six-tuple occurred more than four times as a head, we would have five tail six-tuples at mutual distance $\geqslant 4$, contradicting $A(6, 4) = 4$. So $B(12, 4) \leqslant 4 \times 32 = 128$.

To show $B(12, 4) \geqslant 128$, we construct 128 even-even codewords of distance $\geqslant 4$ analogous to the construction for $B(10, 4)$ in (1) above. Here G_1, a constant-distance 4 linear code, is

000000
111100
001111
110011

(It is the (3, 2) simplex code with columns doubled.) Again there are eight cosets altogether, and the even-even code of length 12 has $8 \times 4 \times 4 = 128$ codewords. The rest is the same as before. So $B(12,4) \geq 128$, and indeed $B(12, 4) = 128$.

(4) $B(12, 8) = 4$. We know $B(12, 8) \leq A(12, 8) = 4$. Here is how to get four even-even twelve-tuples of mutual distance ≥ 8: Use $C(6, 4) = 4$, and write each "1" as "11," each "0" as "00." This doubles the length to 12, doubles the minimum distance to 8, and insures an even number of ones in any even number of consecutive columns starting an odd number of columns from the left, such as column 1 or column 7 with six columns.

This completes verification of all the entries in Table 1 except $B(12, 6) = 20$, which will follow from subsequent results.

III. $B(4n, 2n)$ When n Is Even

First note that if n were even, and there happened to exist, as there usually does, a $2n \times 2n$ Hadamard Matrix H, we could proceed as follows. We can make one row of H all 1's, by reversing columns. Then every row of H has an even number of -1's, either 0 (one row) or n ($2n - 1$ rows). Let H_0 be H under the mapping $1 \rightarrow 0$, $-1 \rightarrow 1$; every row of H_0 has an even number of 1's. The $4n \times 4n$ matrix (or code) given by the well-known tensor product construction

$$H^0_{4n} = \begin{pmatrix} H_0 & H_0 \\ H_0 & \bar{H}_0 \end{pmatrix}$$

is even-even. Here $\bar{H}_0$ is the mod-2 complement of H_0, and is also even.

The distance between any two codewords of H^0_{4n} is found as follows. If their heads are identical, their tails are complementary, and the distance is $2n$. If they both lie in the top or bottom half, the distance is $n + n = 2n$. And if one is in the top half and one in the bottom half with unequal heads, the distance is also $n + n = 2n$. So H^0_{4n} is an even-even Hadamard Matrix, or an even-even code of length $4n$ and distance $2n$. We can now throw in the mod-2 complements of the $4n$ codewords as well, to get an even-even code of length $4n$ with $8n$ codewords of minimum distance $2n$; each word is of distance $4n$ from exactly one other word, its mode-2 complement. This construction shows $B(4n, 2n) \geq 8n$ if n is even and a $2n \times 2n$ Hadamard Matrix exists.

Even without the even-even condition, it is well-known (and easy) that $A(4n, 2n) \leq 8n$ (Ref. 2, p. 43, Cor. 4, or Ref. 3, Thm. 1). Thus $B(4n, 2n) = 8n$ when n is even if a $2n \times 2n$ Hadamard Matrix exists. It is much more difficult to find $B(4n, 2n)$ when n is odd, even if we are willing to assume that convenient Hadamard Matrices exist. We suspect that our upper bound of $8n - 4$ is really the "right" answer, but we have been able to verify it only when $n = 1$ ($B(4, 2) = 4$) and $n = 3$ ($B(12, 6) = 20$). This we start to do in the next section.

IV. $B(4n, 2n)$ When n Is Odd

This section has some preliminary vector space results needed to upper bound $B(4n, 2n)$ when n is odd. The n-odd case is considerably more difficult than the n-even case. We will show that $B(4n, 2n) \leq 8n - 4$ when n is odd. In the following section, we show that the bound is attained when $n = 3$; Table 1 shows that the bound is attained for $n = 1$. Specifically, we solve the following problem in the next few sections:

Problem. Let n be an odd integer, and let $a_1, \cdots, a_k$ be binary codewords of length $4n$. Suppose that each a_i has an even number of 1's among its first $2n$ coordinates. Also suppose $d(a_i, a_j)$ (the Hamming distance between a_i and a_j) is equal to or greater than $2n$ for all $1 \leq i, j \leq k$. Then $k \leq 8n - 4$.

Definition: Let $F = \{f_1, \cdots, f_k\}$ be a collection of vectors in the Euclidean space $\mathbf{R}^s$. Then we say that F satisfies:

Condition (1) if $f_i \neq 0$ and $f_i \cdot f_j \leq 0$, $1 \leq i \neq j \leq k$.

Condition (2) if all coordinates of $f_1, \cdots, f_k$ are ± 1 in some basis of $\mathbf{R}^s$.

Now suppose s is even and F satisfies Condition (2). Fix some basis such that the coordinates of $f_1, \cdots, f_k$ are ± 1 in that basis. Then we can define $w(f_i)$ = the number of 1's among the first $s/2$ coordinates of f_i. We say that F satisfies:

Condition (3) if it satisfies Condition (2), s is even and in some basis of $\mathbf{R}^s$, and $w(f_i)$ is even for all i.

Using this terminology, our problem can be restated in the following way:

Let n be an odd integer. Then if $\{f_1, \cdots, f_k\}$ in $\mathbf{R}^{4n}$ satisfies Conditions (1), (2), and (3), then $k \leq 8n - 4$.

To see that this statement is equivalent to the original problem, replace all zeros by -1's in the binary representation of a_i, and view the resulting $4n$-tuple as a vector f_i in $\mathbf{R}^{4n}$.

V. Some Relevant Facts From Linear Algebra

In this section we shall study the properties of the collections of vectors $F = \{f_1, \cdots, f_k\}$ from $\mathbf{R}^s$ satisfying Condition (1). The underlying space $\mathbf{R}^s$ will play no role in this section, since it can always be replaced by span (F). For this reason we will omit any references to it.

Proposition 1: Let $F = \{f_i, \cdots, f_k\}$ for $k \geqslant 3$ satisfy Condition (1) and suppose the inner product $f_{k-1} \cdot f_k < 0$. Then rank $(f_1, \cdots, f_{k-2}) \leqslant$ rank $(F) - 1$.

Proof: Assume the contrary: $f_1, \cdots, f_{k-2}$ generate $M =$ span (F). Let rank $(F) =$ dim $M = m$. We can assume without loss of generality that $f_1, \cdots, f_m$ is a basis of M. We want to apply the Gram-Schmidt orthogonalization procedure to this basis. Let

$$e_1 = \frac{f_1}{\| f_1 \|}$$

$$e_p = \left(f_p - \sum_{i=1}^{p} (f_p \cdot e_i) e_i \Big/ \left\| f_p - \sum_{i=1}^{p} (f_p \cdot e_i) e_i \right\| \right)$$

for $p = 2, 3, \cdots, m$

We claim that the collection $F_p = \{e_1, e_2, \cdots, e_p, f_{p+1}, \cdots, f_k\}$ satisfies Condition (1) for $p = 1, \cdots, m$.

We induce on p. For $p = 1$ the claim is obvious. Suppose we know it for some $1 \leqslant p \leqslant m$. Then to prove it for $p + 1$ we have to show that

(1) $e_{p+1} \cdot e_i \leqslant 0$ for $i = 1, 2, \cdots, p$.

(2) $e_{p+1} \cdot f_j \leqslant 0$ for $j = p + 2, \cdots, m$.

Here (1) is obvious, since e_{p+1} is orthogonal to e_i by construction. To prove (2), observe that

$$e_{p+1} \cdot f_j = \frac{1}{\left\| f_{p+1} - \sum_{i=1}^{p+1} (f_{p+1} \cdot e_1) e_1 \right\|} \cdot \left(f_p \cdot f_j - \sum_{i=1}^{p} (f_p \cdot e_i)(e_i \cdot f_j) \right)$$

Here

$$f_p \cdot f_j \leqslant 0, f_p \cdot e_i \leqslant 0, e_i \cdot f_j \leqslant 0, i = 1, \cdots, p$$

by our induction assumption. Hence, the expression on the right is nonpositive, as desired. This proves the claim.

Therefore, $\{e_1, \cdots, e_m, f_{m+1}, \cdots, f_k\}$ satisfies Condition (1). By our assumption, f_{k-1}, f_k are in $M =$ span $(e_1, \cdots, e_m)$. Write

$$f_{k-1} = \sum_{i=1}^{m} a_i e_i$$

and

$$f_k = \sum_{i=1}^{m} b_i e_i$$

Then

$$f_{k-1} \cdot e_i \leqslant 0 \text{ implies } a_i \leqslant 0, \ i = 1, \cdots, m$$

$$f_k \cdot e_i \leqslant 0 \text{ implies } b_i \leqslant 0, \ i = 1, \cdots, m$$

From this, we see that

$$0 > f_{k-1} \cdot f_k = \sum_{i=1}^{m} a_i b_i \geqslant 0$$

a contradiction. Therefore, $f_1, \cdots, f_{k-2}$ cannot generate all of M. This proves Proposition 1.

Proposition 1 has the following well-known Corollary, which immediately implies the inequality $A(4n, 2n) \leqslant 8n$ (Ref. 3, Thm. 1). Here we give a proof based on Proposition 1.

Corollary 1: Let $F = \{f_i, \cdots, f_k\}$ satisfy Condition (1) of the previous section. Then $k \leqslant 2$ rank (F).

Proof: We induce on rank (F). When rank $(F) = 1$ the corollary is obvious. Now suppose we know it for rank $(F) = 1, 2, \cdots, m (m \geqslant 1)$, and we want to prove it for rank $(F) = m + 1$. We can assume without loss of generality that $k \geqslant 3$. Suppose $k > 2(m + 1)$. Then clearly $f_i, \cdots, f_k$ cannot be mutually orthogonal; say $f_{k-1} f_k < 0$. Proposition 1 implies rank $(f_1, \cdots, f_{k-2}) \leqslant m$. Hence, by our induction assumption, $k - 2 \leqslant 2$ rank $(F) \leqslant 2m$, i.e., $k \leqslant 2(m + 1)$, a contradiction.

The same argument also proves the following:

Corollary 2: Let $F = \{f_1, \cdots, f_k\}$ satisfy Condition (1), and suppose $k >$ rank (F). Then F contains a subcollection of $k -$ rank (F) mutually orthogonal vectors.

Proposition 2: Let $F = \{f_1, \cdots, f_k\}$, $k > (3/2)\, m = (3/2)$ rank (F) satisfy Condition (1). Then there exists $G = \{g_1, \cdots, g_k\}$ with the following properties:

(1) $g_1, \cdots, g_{k-m}$ are in F and are mutually orthogonal.

(2) $g_{k-m+1} = -g_1, \cdots, g_{3k-4m} = -g_{2k-3m}$.

(3) $g_{3k-4m}, \cdots, g_k$ are in F.

(4) G satisfies Condition (1).

Proof: By Corollary 2 we can assume that $f_1, \cdots, f_{k-m}$ are mutually orthogonal. Choose an orthonormal basis $e_1, \cdots, e_m$ in span (F) such that

$$e_i = \frac{f_i}{\| f_i \|} \text{ for } i = 1, \cdots, k-m$$

Let $f_j = (\alpha_j^1, \cdots, \alpha_j^{k-m}, \cdots, \alpha_j^m)$ in this basis for $k - m + 1 \leqslant j \leqslant k$. Then $f_j \cdot f_1 \leqslant 0, \cdots, f_j \cdot f_{k-m} \leqslant 0$, which implies that for all $k - m + 1 \leqslant j \leqslant k$, $\alpha_j^1, \cdots, \alpha_j^{k-m} \leqslant 0$.

Let $v_j = (\alpha_j^{k-m+1}, \cdots, \alpha_j^m)$. Then

$$v_{j1} \cdot v_{j2} = f_{j1} \cdot f_{j2} - \sum_{i=1}^{k-m} \alpha_{j1}^i \alpha_{j2}^i \geqslant f_{j1} \cdot f_{j2} \geqslant 0$$

Hence, the vectors $\{v_j : j = k - m + 1, \cdots, k\}$ (or those of them that are nonzero, to be precise) satisfy Condition (1). Here rank $\{v_j : j = k - m + 1, \cdots, k\} \leqslant m - (k - m) = 2m - k$. Hence, by Corollary 1, at most $4m - 2k$ of the v_j's are nonzero. So (permuting the f_j's, if necessary), we have the following picture:

$$f_1 = (\| f_i \|, 0, 0, \cdots, 0^{(k-m)}, 0, \cdots, 0)$$

$$f_2 = (0, \| f_2 \|, 0, \cdots, 0, 0, \cdots, 0)$$

$$\vdots$$

$$f_{k-m} = (0, \cdots, \cdots, \cdots, \| f_{k-m} \|, 0, \cdots, 0)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_{k-m+1} = (\beta_1^1, \cdots, \cdots, \cdots, \beta_1^{(k-m)}, 0, \cdots, 0)$$

$$\vdots$$

$$f_{3k-4m} = (\beta_{2k-3m}^1, \cdots, \cdots, \beta_{2k-3m}^{(k-m)}, 0, \cdots, 0)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_{3k-4m+1} = (\gamma_1^1, \cdots, \cdots, \cdots, \gamma_1^{(k-m)}, \nu_1)$$

$$\vdots$$

$$f_k = (\gamma_{4m-2k}^1, \cdots, \cdots, \gamma_{4m-2k}^{(k-m)}, \nu_{4m-2k})$$

Here, as we showed above, all β_j^i and γ_j^i are $\leqslant 0$.

We claim the following. Suppose $\beta_j^i < 0$ for some $1 \leqslant i \leqslant k - m$, $1 \leqslant j \leqslant 2k - 3m$. Then every other β and every other γ in the ith column must be equal to 0. Indeed, suppose $\gamma_s^i < 0$ for some s. Then

$$0 \geqslant f_j \cdot f_s = \sum_{t=1}^{k-m} \beta_j^e \gamma_s^e > 0$$

(the ith term is > 0 and the other terms are all $\geqslant 0$) and we get a contradiction. The same argument shows that $\beta_s^i = 0$ for $s \neq j$.

Now, since each f_j has at least one nonzero coordinate, we can assume that $\beta_1^1 \neq 0, \beta_2^2 \neq 0, \cdots, \beta_{2k-3m}^{2k-3m} \neq 0$. Then our claim proves that the collection $\{f_1, \cdots, f_{k-m}, -f_1, \cdots, -f_{2k-3m}, f_{3k-4m+1}, \cdots, f_k\}$ satisfies Condition (1). This proves Proposition 2.

VI. Linear Dependence of (-1, 1) Vectors

In this section we shall study the collections $F = \{f_1, \cdots f_k\}$ of $\mathbf{R}^s$ satisfying Condition (2). Some elementary lemmas are in order.

Lemma 1: Let $A = (a_{ij})$ be an $n \times n$ matrix with all $a_{ij} = \pm 1$. Then

(1) If $n = 2$, $\det A = 0, \pm 2$.

(2) If $n = 3$, $\det A = 0, \pm 4$.

(3) If $n = 4$, $\det A = 0, \pm 8, \pm 16$.

Proof: If we subtract the first row of A from the other $n - 1$, then the last $n - 1$ rows will have entries $0, \pm 2$. This shows that $\det A$ is divisible by 2^{n-1}. On the other hand, if we denote the row vectors of A by $a_1, \cdots, a_n$ then $|\det A| \leqslant \| a_1 \| \cdot \| a_2 \| \cdots \| a_n \|$ (because $|\det A|$ = measure of the n-parallelopiped spanned by the a_i) $= (\sqrt{n})^n$. Combining these two properties ($2^{n-1} \mid \det A$ and $|\det A| \leqslant (\sqrt{n})^n$) we get (1), (2), and (3). This proves Lemma 1.

We recall the following standard terminology:

Definition: $F = \{f_1, \cdots, f_k\}$ is *minimally linearly dependent* if F is linearly dependent but any proper subcollection of F is linearly independent.

Clearly if F is minimally linearly dependent, then k = rank $(F) + 1$. We can now prove Lemma 2.

Lemma 2: Suppose $F = \{f_1, \cdots, f_k\}$ satisfies Condition (1) of Section 4 (nonpositive inner product). Then if

(1) Rank $(F) = 1$ with $k = 2$, F is minimally linearly dependent if and only if $f_1 = -f_2$;

(2) Rank $(F) = 2$, F cannot be minimally linearly dependent;

(3) Rank $(F) = 3$ with $k = 4$, F is minimally linearly dependent if and only if $f_1 = k_2 f_2 + k_s f_s + k_4 f_4$ with $k_i = \pm 1$ for $i = 2, 3, 4$;

(4) Rank $(F) = 4$ with $k = 5$, F is minimally linearly dependent if and only if $k_1 f_1 = k_2 f_2 + \cdots + k_5 f_5$ with k_i chosen from $\{\pm 1, \pm 2\}$.

Proof: (1) is obvious. If F satisfies Condition (2) and is minimally linearly dependent, then we can write f_1 as

$$\sum_{i=2}^{k} \alpha_i f_i, \quad \alpha_i \neq 0, \quad \text{all } i$$

In coordinates (using the basis that represents the f_i's as (-1, 1) vectors), if $f_i = (f_i^1, \cdots, f_i^s)$, $f_i^j = \pm 1$, this equality becomes the system of linear equations

$$\sum_{i=2}^{k} \alpha_i f_s^i = f_1^i, \quad j = 1, 2, \cdots, s$$

Since F is minimally linearly dependent,

$$\operatorname{rank} (f_s^i)_{\substack{i=2,\cdots,k \\ j=1,\cdots,s}} = k - 1$$

and the α_i can be computed (using Cramer's rule) as ratios of the determinants of two $(k - 1) \times (k - 1)$ matrices whose entries are f_s^i, i.e., $= \pm 1$. Since F is minimally linearly dependent, none of the α_i's can be 0. Thus Lemma 1 gives (3) and (4).

To prove (2), observe that by Lemma 1, the only possibility is $\alpha_1, \alpha_2 = \pm 1$, i.e., $f_1 = \pm f_2 \pm f_s$. The entries of $\pm f_2 \pm f_s$ have to be 0, ± 2, and the entries of f_1 are ± 1. This proves (2).

Lemma 3: Let $F = \{f_1, \cdots, f_k\}$ satisfy conditions (1) and (2) and be minimally linearly dependent with rank $F = m$. Then

(1) If $m = 3, k = 4$, then $f_1 + f_2 + f_s + f_4 = 0$;

(2) If $m = 4$, $k = 5$ then $k_1 f_1 + k_2 f_2 + \cdots + k_5 f_5 = 0$ with $k_1, \cdots, k_5$ chosen from $\{1, 2\}$.

Proof: (1) Assume the contrary. Lemma 2 says that $k_1 f_1 + k_2 f_2 + k_3 f_3 + k_4 f_4 = 0$, where $k_1, k_2, k_3, k_4 = \pm 1$. We can assume without loss of generality that $k_1 = k_2 = 1$, $k_4 = -1$. Taking the inner product of both sides with f_4, we get $f_1 \cdot f_4 + f_2 \cdot f_4 + k_3 f_3 \cdot f_4 - f_4 \cdot f_4 = 0$. But $f_4 \cdot f_4 = s$, while $f_1 \cdot f_4$, $f_2 \cdot f_4 < 0$. Hence, $k_3 (f_3 \cdot f_4) - s \geqslant 0$ so $|f_3 \cdot f_4| \geqslant s$. But $\|f_s\| = \|f_4\| = \sqrt{s}$. Hence, $|f_s \cdot f_4| \leqslant s$, with equality if and only if $f_4 = -f_3$. Since we assumed that $\{f_1, \cdots, f_4\}$ is minimally linearly dependent, this is impossible. This proves (1).

(2) Again, assume the contrary. Lemma 2 says that

$$\sum_{i=1}^{5} k_i f_i = 0 \text{ with } k_i \text{ chosen from } \{\pm 1, \pm 2\}$$

We can assume without loss of generality that $k_1, k_2, k_3 > 0$, $k_5 < 0$. If $k_4 > 0$, then take the inner product of

$$\sum_{i=1}^{5} k_i f_i = 0$$

with f_5 to get a contradiction.

If $k_4 < 0$ then we can assume without loss of generality that $|k_4| \geqslant |k_5|$. Then taking the inner product of both sides with f_4, we get

$$k_4 s + k_5 (f_4 \cdot f_5) \geqslant 0, \quad \text{i.e., } |k_4| s \leqslant |k_5| \cdot |f_4 \cdot f_5|$$

This implies

$$|f_4 \cdot f_5| \geqslant s$$

and the same argument as in (1) leads to a contradiction.

Corollary 1. Let $F = \{f_1 \cdots, f_k\}$ satisfy Conditions (1) and (2).

(1) If $\{f_1, f_2\}$ are minimally linearly dependent, then f_i is orthogonal to f_j for $i = 1, 2, j = 3, \cdots, k$.

(2) If $\{f_1, \cdots, f_4\}$ are minimally linearly dependent, then f_i is orthogonal to f_j for $i = 1, 2, \cdots, 4$, $j = 5, \cdots, k$.

(3) If $\{f_1, \cdots, f_5\}$ are minimally linearly dependent, then f_i is orthogonal to f_j for $i = 1, \cdots, 5, j = 6, \cdots, k$.

Proof: In (2), by Lemma 3, $\Sigma_{i=1}^{4} f_i = 0$. Hence, for $j \geqslant 5$,

$$0 = f_j \cdot \left(\sum_{i=1}^{4} f_i\right) = \sum_{i=1}^{4} (f_j \cdot f_i)$$

Each term $(f_j \cdot f_i)$ is nonpositive. Hence, the above equality implies that they all must be 0. This proves (2). The same argument proves (1) and (3) (in (1), $f_1 + f_2 = 0$).

Corollary 2: Let $F = \{f_1, \cdots, f_k\}$ of $\mathbf{R}^s$ satisfy Conditions (1) and (2), and let m = rank (F).

(1) If $m = 3$, $k = 4$ and f_2, f_3, and f_4 are mutually orthogonal, then F cannot be minimally linearly dependent.

(2) If $m = 4$, $k = 5$, and f_2, f_3, f_4, f_5 are mutually orthogonal with F minimally linearly dependent, then $f_1 = k_2 f_2 + \cdots + k_5 f_5$ with $k_2, \cdots, k_5 = \pm 1/2$.

Proof. To prove (1), observe that by Lemma 2, $f_1 = k_2 f_2 + k_3 f_3 + k_4 f_4$ where $k_2, k_3, k_4 = \pm 1$. Then

$$s = f_1 \cdot f_1 = \left\| \sum_{i=2}^{4} k_i f_i \right\|^2 = \sum_{i=2}^{4} k_i^2 \| f_i \|^2 = \sum_{i=2}^{4} s = 3s$$

a contradiction. To prove (2), by Lemma 2, we can write f_1 as $\Sigma_{i=2}^{5} k_i f_i$ where the k_i are chosen from $\{\pm 1/2, \pm 1, \pm 2\}$. Now

$$s = \| f_1 \|^2 = \sum_{i=2}^{5} k_i^2 \| f_i \|^2 = \left(\sum_{i=1}^{5} k_i^2\right) s$$

Hence, $\Sigma_{i=2}^{5} k_i^2 = 1$, which proves (2).

VII. Maximal Orthogonal Systems Satisfying Condition (3)

The question of the existence of an orthogonal basis F of $\mathbf{R}^5$ satisfying Condition (2) is the question of existence of an $s \times s$ Hadamard Matrix. In this section we shall prove that when $s = 4n$, n odd, no basis of $\mathbf{R}^s$ can satisfy Condition (3), i.e., s odd, weights even. Moreover, any orthogonal system F satisfying Condition (3) can have at most $s - 2$ vectors (Proposition 3 below). To prove this result, we need the following Lemma from Ref. 4, stated here without proof.

Lemma 4: Let $f_1, \cdots, f_{4n-\alpha}$ be mutually orthogonal $(1, -1)$ vectors in $\mathbf{R}^{4n}$. Then if $\alpha = 1$, 2 or 3, there exist α more $(1, -1)$ vectors $g_1, \cdots, g_\alpha$ such that $\{f_1, \cdots, f_{4n-\alpha}, g_1, \cdots, g_\alpha\}$ is an orthogonal basis of $\mathbf{R}^{4n}$.

Proposition 3: Let $F = \{f_1, \cdots, f_{4n-1}\}$ satisfy Conditions (1), (2), and (3). Then the vectors $f_1, \cdots, f_{4n-1}$ cannot be mutually orthogonal.

Proof. Assume the contrary. Then by Lemma 4 there exists a $(-1, 1)$ vector f_{4n} such that $\{f_1, \cdots, f_{4n-1}, f_{4n}\}$ is an orthogonal basis of $\mathbf{R}^{4n}$. Let $w_i = w(f_i)$ for $i = 1, \cdots, 4n$. By our assumption, w_i is even for $i = 1, \cdots, 4n - 1$. Consider the vector $c = (1, 1, \cdots, 1^{(2n)}, 0, \cdots, 0)$ (in the original basis). Then $c \cdot f_i = 2(n - w_i)$ and $\| f_i \|^2 = 4n$. Hence,

$$c = \sum_{i=1}^{4n} \frac{2(n - w_i)}{4n} f_i$$

Knowing this, we see that

$$2n = \| c \|^2 = \left\| \sum_{i=1}^{4n} \frac{n - w_i}{2n} f_i \right\|^2$$

$$= \sum_{i=1}^{4n} \frac{(n - w_i)^2}{4n^2} \cdot \| f_i \|^2$$

$$= \sum_{i=1}^{4n} = \frac{(n - w_i)^2}{n}$$

Therefore,

$$2n^2 = \sum_{i=1}^{4n} (n - w_i)^2$$

Now we reduce this equality mod 4. Because n is odd, $2n^2 \equiv 2 \bmod 4$. Similarly $n - w_i$ is odd for $i = 1, \cdots, 4n - 1$. Hence,

$$\sum_{i=1}^{4n-1} (n - w_i)^2 \equiv 4n - 1 \equiv -1 \bmod 4$$

This leaves us with

$$(n - w_{4n})^2 \equiv 3 \bmod 4$$

which is impossible, since $a^2 \equiv 0$ or $1 \bmod 4$ for any integer a. This contradiction completes the proof of Proposition 3.

VIII. The Main Theorem

We now have the necessary tools to upper bound $B(4n, 2n)$ when n is odd. We start with another lemma.

Lemma 5. Suppose $F = \{f_1, \cdots, f_{5n-3}\}$ of $\mathbf{R}^{4n}$ (n odd) satisfies Conditions (1), (2), and (3). Then F cannot have a minimally linearly dependent subset of four elements.

Proof: Suppose f_{8n-6}, f_{8n-5}, f_{8n-4}, and f_{8n-3} are minimally linearly dependent. Denote their span by M. By definition, dim $M = 3$. Then by Corollary 1 (2) to Lemma 3, $f_1, \cdots, f_{8n-7}$ are in M^{perp}. Hence, rank $\{f_1, \cdots, f_{8n-7}\} \leqslant 4n - 3$. By Proposition 2 (with $k = 8n - 7$, $m = 4n - 3$), we can assume (replacing $\{f_1, \cdots, f_{8n-7}\}$ by G if necessary) that $f_1, \cdots, f_{4n-5(=2k-3m)}$ are mutually orthogonal and $f_{4n-6} = -f_1, \cdots, f_{8n-10} = -f_{4n-5}$. Then Corollary 1 (1) to Lemma 3 forces $f_{8n-9}, f_{8n-8}, f_{8n-7}$ to be in (span $(f_1, \cdots, f_{4n-5})^{perp}$). That is, rank $(f_{8n-9}, f_{8n-8}, f_{8n-7}) \leqslant 2$.

By Lemma 2 (2), (1) we can thus assume that $f_{8n-8} = -f_{8n-9}$, which again forces f_{8n-7} and f_{8n-9} to be orthogonal. Therefore, $F = \{f_1, \cdots, f_{4n-5}, f_{8n-9}, f_{8n-7}, f_{8n-6}\}$ is an orthogonal system satisfying Condition (2) and containing $4n - 2$ vectors. Hence, by Lemma 4 there exist (-1, 1) vectors h_1 and h_2 such that F with h_1 and h_2 adjoined is an orthgonal basis of $\mathbf{R}^{4n}$. Since f_{8n-5} is orthogonal to f_i for $i = 1, \cdots, 8n - 7$, we have that f_{8n-5} is in span $\{f_{8n-6}, h_1, h_2\}$. Then by Corollary 2(1) to Lemma 3, $\{f_{8n-5}, f_{8n-6}, h_1, h_2\}$ cannot be minimally linearly dependent, i.e., it must have a pair of opposites.

But $f_{8n-5} = -h_i$ ($i = 1$ or 2) is impossible because then $\{f_1, \cdots, f_{4n-5}, f_{8n-7}, f_{8n-6}, f_{8n-5}\}$ would be an orthogonal system of $4n - 1$ (-1, 1) vectors, contradicting Proposition 3. And $f_{8n-5} = -f_{8n-6}$ contradicts our assumption about minimal linear dependence of f_{8n-6}, f_{8n-5}, f_{8n-4}, and f_{8n-3}. And, finally, there cannot be any opposites among $\{f_{8n-6}, h_1, h_2\}$ because these vectors are mutually orthogonal. This contradiction proves Lemma 5.

Lemma 6. Suppose $F = \{f_1, \cdots, f_{8n-3}\}$ of $\mathbf{R}^{4n}$ (n odd) satisfies Conditions (1), (2), and (3). Then F cannot have a minimally linear dependent subset of 5 elements.

Proof: We use the same strategy. Assume the contrary, say $f_{8n-7}, f_{8n-6}, \cdots, f_{8n-3}$ are minimally linearly dependent. Let M = span $\{f_{8n-7}, \cdots, f_{8n-3}\}$, dim $(M) = 4$. Then $f_1, \cdots, f_{8n-8} \in M^{perp}$ by Corollary 1(3) to Lemma 3. Hence, rank $\{f_1, \cdots, f_{8n-8}\} \leqslant 4n - 4$. Then by Corollary 2 to Proposition 1 we can assume that $f_1, \cdots, f_{4n-4}$ are mutually orthogonal. Then $\{f_1, \cdots, f_{4n-4}, f_{8n-7}\}$ is an orthogonal system of $4n - 3$ vectors. By Lemma 4 there exist three (-1, 1) vectors h_1, h_2, and h_3 such that $\{f_1, \cdots, f_{8n-7}, h_1, h_2, h_3\}$ is an orthogonal basis of $\mathbf{R}^{4n}$.

Note that f_{8n-7}, f_{8n-6}, f_{8n-5}, f_{8n-4}, f_{8n-3} are in span $\{f_{8n-7}, h_1, h_2, h_3\}$. We claim that there is an orthogonal pair among $\{f_{8n-7}, \cdots, f_{8n-3}\}$. For proof assume the contrary: $f_1 \cdot f_j < 0$ for all $i \neq j$ in $\{8n - 7, \cdots, 8n - 3\}$. Denote f_{8n-8+i} by g_i for $i = 1, \cdots, 5$. For $i = 2, 3, 4, 5$ write g_i as

$$\alpha_i g_1 + \sum_{j=1}^{3} \beta_i^j h_j$$

Since $\alpha_i = (g_i \cdot g_1)/4n$, it must be negative by our assumption, for $i = 2, 3, 4, 5$. On the other hand, $\alpha_i \neq -1$, because we assume that $\{g_i : i = 1, 2, \cdots 5\}$ is minimally linearly dependent. Hence, by Corollary 2 to Lemma 3 and Lemma 2 (2), $\alpha_i = -1/2$, $\beta_i^j = \pm 1/2$ for all i, j.

We can assume without loss of generality that β_2^2 and β_2^3 have the same sign. Then

$$0 > \frac{g_2 \cdot g_3}{4n} = \frac{\left(-\frac{1}{2}g_1 + \sum_{j=1}^{3} \beta_2^j h_j\right) \cdot \left(-\frac{1}{2}g_1 + \sum_{j=1}^{3} \beta_3^j h_j\right)}{4n}$$

$$= \left(\frac{1}{4} + \beta_2^1\beta_3^1\right) + \left(\beta_2^2\beta_3^2 + \beta_2^3\beta_3^3\right)$$

$$= \frac{1}{2} + \left(\beta_2^2\beta_3^2 + \beta_2^3\beta_3^3\right)$$

$$\geqslant \frac{1}{2} + \left(-\frac{1}{4} - \frac{1}{4}\right) = 0$$

a contradiction. This contradiction proves the claim.

Now (using the same notation as in the proof of the claim) we can assume that g_1 and g_2 are orthogonal. By Lemma 4, we can complete the orthogonal system $\{f_1, \cdots, f_{4n-4}, g_1, g_2\}$ to an orthogonal basis by adding two new (-1, 1) vectors t_1 and t_2. Write

$$g_i = p_i^1 g_1 + p_i^2 g_2 + p_i^3 t_1 + p_i^4 t_2$$

By Corollary 2 to Lemma 3 and Lemma 2, for each i, there are only two possibilities for the p_i^j's:

(1) One of the coefficients $p_i^1, p_i^2, p_i^3, p_i^4$ is ± 1 and the other three are 0;

(2) $p_i^1, \cdots, p_i^4 = \pm 1/2$.

Let us consider each of these two possibilities.

(1) p_i^1, p_i^2 cannot be ± 1, since we assume that $\{g_1, \cdots, g_5\}$ are minimally linearly dependent. If $p_i^3 = \pm 1$ then

$\{f_1, \cdots, f_{4n-4}, g_1, g_2, g_i\}$ would be an orthogonal system of $4n - 1$ (-1, 1) vectors, contradicting Proposition 3. Similarly $p_i^4 \neq \pm 1$. Thus (1) is impossible for any $i = 3, 4, 5$.

(2) In this case $p_i^1 = p_i^2 = -1/2$, since

$$p_i^j = \frac{g_i \cdot g_j}{4n} \leqslant 0 \text{ for } i = 3, 4, 5, j = 1, 2$$

We can assume without loss of generality that β_3^3 and β_3^4 have the same sign. Then

$$\frac{g_3 \cdot g_4}{4n} = \left(-\frac{1}{2}g_1 - \frac{1}{2}g_2 + \beta_3^3 t_1 + \beta_3^4 t_2\right)$$

$$\cdot \left(-\frac{1}{2}g_1 - \frac{1}{2}g_2 + \beta_4^4 t_1 + \beta_4^4 t_2\right)$$

$$= \left(\frac{1}{4} + \frac{1}{4} + \beta_3^3\beta_3^4\right) + \beta_4^4\beta_3^4 = \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) + \beta_4^4\beta_3^4$$

$$\geqslant \frac{3}{4} - \frac{1}{4} = \frac{1}{2} > 0$$

This contradiction proves Lemma 6.

Now we at last reach the main theorem of this paper.

Theorem: Suppose $F = \{f_1, \cdots, f_k\}$ of $\mathbf{R}^{4n}$ (n odd) satisfies Conditons (1), (2), and (3). Then $k \leqslant 8n - 4$. That is, $B(4n, 2n) \leqslant 8n - 4$ (n odd).

Proof: It is sufficient to prove that $F = \{f_1, \cdots, f_{8n-3}\}$ cannot satisfy Conditions (1), (2), and (3). Assume the contrary. Then by Proposition 2, we can assume (replacing F by G if necessary) that $f_1, \cdots, f_{4n-6}$ are mutually orthogonal and $f_{4n-5} = -f_1, \cdots, f_{8n-12} = -f_{4n-6}$ (here $k = 8n - 3, m \leqslant 4n$). By Corollary 2 (1), the remaining nine vectors (denote them by $g_1, \cdots, g_9$; $g_i = f_{8n-12+i}$) lie in the orthogonal complement of span $\{f_1, \cdots, f_{4n-6}\}$. Hence, rank $\{g_1, \cdots, g_9\} \leqslant 6$. So $g_1, \cdots, g_9$ cannot be mutually orthogonal, and we can assume that $g_1 \cdot g_2 < 0$.

By Proposition 1, we can now conclude that rank $\{g_3, \cdots, g_9\} \leqslant 5$. Again (permuting the g_i's if necessary, we can assume that $g_3 \cdot g_4 < 0$. Then by Proposition 1, rank $\{g_5, \cdots, g_9\} \leqslant 4$. By Lemma 6, $\{g_5, \cdots, g_9\}$ cannot be minimally linearly dependent. By Lemma 5, no subcollection of this collection containing four elements can be minimally linearly dependent. By Lemma 2 (2), no subcollection of three elements can be minimally linearly dependent.

All this means that $\{g_5, \cdots, g_9\}$ contains a pair of opposites, say $g_8 = -g_9$. Then by Corollary 1 (1) to Lemma 3, g_i is orthogonal to g_8 for $i = 1, \cdots, 7$. Hence, rank $\{g_3, \cdots, g_7\} \leqslant 4$. Using the same argument as above, we see that the collection $\{g_3, \cdots, g_7\}$ must contain a pair of opposites, say $g_6 = -g_7$. By Corollary 1 (1) to Lemma 3, g_i is orthogonal to g_6 for $i = 1, \cdots, 5$. Hence, rank $\{g_1, \cdots, g_5\} \leqslant 4$.

Again Lemmas 5, 6, and 2 (2) imply that this collection, too, must contain a pair of opposites, say $g_4 = -g_5$. But then by Corollary 2 (1) to Lemma 3, g_1, g_2, and g_3 are orthogonal to g_4. Therefore, $\{f_1, \cdots, f_{4n-6}, g_2, g_4, g_6, g_8\}$ is an orthogonal collection of $4n - 2$ (-1, 1) vectors. By Lemma 4, there exist (-1, 1) vectors h_1 and h_2 such that $\{f_1, \cdots, f_{4n-6}, g_2, g_4, g_6, g_8, h_1, h_2\}$ is an orthogonal basis of $\mathbf{R}^{4n}$.

Since g_1 is orthogonal to $f_1, \cdots, f_{4n-6}$, then g_4, g_6, g_8, g_1 must all lie in span $\{g_2, h_1, h_2\}$. Since g_2, h_1, and h_2 are mutually orthogonal, Corollary 2 (1) to Lemma 3 says that g_1, g_2, h_1, and h_2 cannot be minimally linearly dependent. Then by Lemma 2 (2), (1), this collection must have a pair of opposites. Since g_2, h_1, and h_2 are mutually orthogonal, there are only two possibilities, each of which we rule out:

(1) $g_1 = -g_2$. Then by Corollary 2 (1) to Lemma 3, every other vector in the original collection will be orthogonal to g_1 and g_2. Hence, $\{f_1, \cdots, f_{4n-6}, g_2, g_4, g_6, g_8, g_3\}$ will be an orthogonal collection of $4n - 1$ vectors, contradicting Proposition 3.

(2) $g_1 = -h_i$ ($i = 1$ or 2). Then $\{f_1, \cdots, f_{4n-6}, g_1, g_2, g_4, g_6, g_8\}$ will be an orthogonal collection, which again contradicts Proposition 3. This contradiction at last proves the Theorem: $B(4n, 2n) \leqslant 8n - 4$ if n is odd.

IX. Determining $B(12, 6)$

We have left determination of $B(12, 6)$ to the end, because we need the upper bound $B(12, 6) \leqslant 8 \cdot 3 - 4 = 20$ of the preceding section. Table 2 is a particular code meeting the upperbound, showing that $B(12, 6) = 20$.

This example has some additional structure that helped us find it and that may generalize. Note that $A_2, \cdots, A_{10}$ are at distance 4 from A = (000000111111). Also note that $A_{k+10} = A_k$, $1 \leqslant k \leqslant 10$. It may be that whenever $B(4n, 2n) = 8n - 4$ with n odd, the code consists of $4n - 2$ orthogonal vectors and their complements. We can now readily check by inspection that for $k < m$, $1 \leqslant k \leqslant 10$,

$$d(A_k, A_m) = \begin{cases} 12 & \text{if } m - k = 9 \ (2 \leqslant k \leqslant 10) \text{ or } k = 1, m = 20; \\ 6 & \text{otherwise.} \end{cases}$$

so that the code of Table 2 has minimum distance 6.

Some additional structure that helped us find the code is as follows. If we consider the middle 18 rows of Table 2 as decomposed into four 9-row by 6-column blocks, there are three 1's in each column of the two diagonal blocks, each of which consists of six-tuples of weight 2, and six 1's in each column of the antidiagonal blocks. One can show in the case $n = 3$ that, once we know that there is a pair of codewords at distance 12, all the additional structure follows. Knowing all this, Table 2 was easy to derive.

References

1. Posner, Edward C., and Zinvoy Reichstein, "Minimum-Distance Problems in Protocol Design," TDA Progress Report 42-77, January-March 1984. Jet Propulsion Laboratory, Pasadena, California.
2. MacWilliams, F. J., and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.
3. Rankin, R. A., "The Closest Packing of Spherical Caps in n Dimensions," *Proc. Glasgow Math. Assoc.*, Vol. 2 (1955), pp. 139-144.
4. Hall, Marshall, and Herbert J. Ryser, "Normal Completions of Incidence Matrices," *Amer. Jour. Math.*, Vol. 76 (1954), pp. 581-589.

Table 1. Largest codes[a] of even lengths $2k \leq 12$

$2k = 2$			
d	$A(2,d)$	$C(2,d)$	$B(2,d)$
1	4	2	1
2	2	2	1

$2k = 4$			
d	$A(4,d)$	$C(4,d)$	$B(4,d)$
1	16	8	4
2	8	8	4
3	2	2	2
4	2	2	2

$2k = 6$			
d	$A(6,d)$	$C(6,d)$	$B(6,d)$
1	64	32	16
2	32	32	16
3	8	4	4
4	4	4	4
5	2	2	1
6	2	2	1

$2k = 8$			
d	$A(8,d)$	$C(8,d)$	$B(8,d)$
1	256	128	64
2	128	128	64
3	20	16[b]	16[b]
4	16	16[b]	16[b]
5	4	2	2
6	2	2	2
7	2	2	2
8	2	2	2

$2k = 10$			
d	$A(10,d)$	$C(10,d)$	$B(10,d)$
1	1024	512	256
2	512	512	256
3	72-80	38-40[c]	32[d]
4	38-40	38-40[c]	32[d]
5	12	6[c]	5[d]
6	6	6[c]	5[d]
7	2	2	2
8	2	2	2
9	2	2	1
10	2	2	1

$2k = 12$			
d	$A(12,d)$	$C(12,d)$	$B(12,d)$
1	4096	2048	1024
2	2048	2048	1024
3	256	144-160[e]	128[d]
4	144-160	144-160[e]	128[d]
5	32	24[e]	20[f]
6	24	24[e]	20[f]
7	4	4[g]	4[d]
8	4	4[g]	4[d]
9	2	2	2
10	2	2	2
11	2	2	2
12	2	2	2

A: unconstrained,
C: even
B: even-even.

[a] A-Values from Ref. 2, App. A, p. 674, Fig. 1.
[b] Biorthogonal (8, 4) linear codewords for $C(8, 4)$ $(= C(8, 3)) = B(8, 4) = 16$.
[c] From Ref. 2, $A(9, 5) = 6$, and append an even parity bit; likewise $38 \leq A(9, 3) \leq 40$.
[d] Derived in this Section: $B(2k, 2t - 1) = B(2k, 2t)$ because all distances are even.
[e] Same reasoning as footnote c, where $144 \leq A(11, 3) \leq 160$, $A(11, 5) = 24$.
[f] Derived in Section 9.
[g] Use $B(12, 8) = 4$.

Table 2. $B(12, 6) \geq 20$

	$A_k(1)$						$A_k(2)$					
A_1	0	0	0	0	0	0	0	0	0	0	0	0
A_2	0	0	1	0	0	1	1	1	1	1	0	0
A_3	0	1	0	0	0	1	1	1	0	0	1	1
A_4	1	0	0	0	0	1	0	0	1	1	1	1
A_5	0	0	1	0	1	0	1	0	1	0	1	1
A_6	0	1	0	0	1	0	0	1	1	1	1	0
A_7	1	0	0	0	1	0	1	1	0	1	0	1
A_8	0	0	1	1	0	0	0	1	0	1	1	1
A_9	0	1	0	1	0	0	1	0	1	1	0	1
A_{10}	1	0	0	1	0	0	1	1	1	0	1	0
A_{11}	1	1	0	1	1	0	0	0	0	0	1	1
A_{12}	1	0	1	1	1	0	0	0	1	1	0	0
A_{13}	0	1	1	1	1	0	1	1	0	0	0	0
A_{14}	1	1	0	1	0	1	0	1	0	1	0	0
A_{15}	1	0	1	1	0	1	1	0	0	0	0	1
A_{16}	0	1	1	1	0	1	0	0	1	0	1	0
A_{17}	1	1	0	0	1	1	1	0	1	0	0	0
A_{18}	1	0	1	0	1	1	0	1	0	0	1	0
A_{19}	0	1	1	0	1	1	0	0	0	1	0	1
A_{20}	1	1	1	1	1	1	1	1	1	1	1	1